Remcoh
Voordelig en compleet ICT-beheer

Hoe veilig zijn mijn gegevens in Office 365?

Remcoh legt uit

In deze white paper vijf vragen die belangrijk zijn om jezelf te stellen voordat je besluit om jouw gegevens online te plaatsen:

1. Waar staan mijn gegevens?
2. Blijf ik eigenaar van mijn gegevens?
3. Hoe belangrijk is de beveiliging en jouw privacy voor de service provider?
4. Welke maatregelen zijn genomen om de beveiliging en privacy te waarborgen?
5. Welke mogelijkheden krijg ik zelf voor beveiliging en controle?

De antwoorden op de vraag 1 t/m 5 zijn ingevuld met het antwoord van Microsoft over Office 365. Als laatste geven wij een antwoord op de vraag (nummer 6): Hoe veilig zijn mijn gegevens in Office 365?

1. Waar staan mijn gegevens?

Meer precies; in welk landen staan mijn gegevens en hoe veilig zijn mijn gegevens in die landen? Let bijvoorbeeld op de invloed van de overheid van dat land op de veiligheid en privacy van jouw gegevens. Hoe goed ben je beschermd door wetgeving?

Microsoft bewaart de gegevens van Europese klanten van Office 365 in Ierland en Nederland. Je bent hierdoor beschermd door de wetgeving van de EU. Het feit dat Microsoft het hoofdkantoor in Amerika heeft, geeft de Amerikaanse overheidsinstanties niet het recht om jouw gegevens te krijgen. De instantie moet met hele goede redenen komen bij de Europese rechter om achter bepaalde gegevens te komen.

2. Blijf ik eigenaar van mijn gegevens?

Neem goed de voorwaarden van de service provider door voordat je akkoord gaat. In veel gevallen mag de partij een deel van jouw gegevens gebruiken en in bepaalde gevallen worden zij eigendom van de gegevens die je bij hen opslaat. Uiteraard met goede bedoelingen, maar het feit is dat je andere bedoelingen onvoldoende kan controleren. Het is een afweging tussen dit risico en de extra kwaliteit of kostenvoordeel van de service die je ervoor terugkrijgt.

Microsoft is hier heel stellig in. Jij blijft eigenaar van jouw gegevens in Office 365 en Microsoft biedt het Office 365 platform aan als dienst, zonder interesse in gegevens.

3. Hoe belangrijk is de beveiliging en jouw privacy voor de service provider?

Bepaalde partijen hebben er juist baat bij om jouw gegevens te gebruiken voor promotie en advertenties. Jouw identiteit is geld waard. Zij kunnen hun diensten gratis aanbieden, omdat ze hun inkomsten krijgen uit andere middelen zoals adverteerders. Andere aanbieders van bijvoorbeeld Open Source zien beveiliging als hindernis en willen juist informatie delen zodat iedereen er beter van wordt, niet zozeer jij als individu.

Microsoft respecteert jouw privacy en verzamelt niet jouw gegevens in Office 365 voor advertenties. Microsoft krijgt de inkomsten voor Office 365 uit het abonnement. Door deze inkomsten kan Microsoft een veilig Office 365 platform bieden.

4. Welke maatregelen zijn genomen om de beveiliging en privacy te waarborgen?

De online omgeving dient op drie vlakken beveiligd te zijn: Beveiliging tegen internetaanvallen, fysieke beveiliging en een beveiligde verbinding naar de gebruiker. Het is ook belangrijk dat dit gecontroleerd wordt door een derde onafhankelijke keuringsinstantie als waarborg.

Microsoft werkt vanaf het ontwerp van Office 365 continu aan beveiliging en bescherming van de privacy van de omgeving. Dit is gericht op het voorkomen, detecteren en weerleggen van aanvallen van buiten en van binnen. De e-mail van de klanten wordt ook standaard continu beschermd tegen virussen en spam.

De datacenters waar de Office 365 omgeving draait worden 24 uur per dag bewaakt tegen inbraak en calamiteiten. Hierop wordt streng gecontroleerd door onder andere beveiligingspersoneel, videobewaking, inbraakalarmsystemen en pascontrole.

De Office 365 omgevingen van de verschillende klanten zijn gescheiden. Iedere gebruiker heeft toegang tot zijn gegevens via een versleutelde verbinding en met een verplicht sterk wachtwoord. De verbinding tussen de datacenters is ook versleuteld.

Onafhankelijke instanties controleren op naleving van het beveiliging- en privacy-beleid voor Office 365 door Microsoft. Ze zijn onder andere gecertificeerd voor ISO 27001. Dit is een ISO standaard voor informatiebeveiliging, waar bijvoorbeeld Nederlandse overheidsinstanties aan moeten voldoen.

5. Welke mogelijkheden krijg ik zelf voor beveiliging en controle?

In de basis moet de omgeving gewoon goed beveiligd zijn. Het gaat er juist om welke mogelijkheden je krijgt om zelf extra beveiliging en controle te krijgen die jij nodigt vindt om jouw gegevens te beschermen. Of juist andersom, de omgeving meer toegankelijk en werkbaar maken voor de gebruikers.

In Office 365 krijg je als beheerder de mogelijkheid om de beveiliging en privacy instellingen strakker en losser in te stellen per gebruiker, rol, groep en de gehele organisatie. Je kan ook beheer van verschillende onderdelen delegeren. Je hebt zelfs de mogelijkheid om de gegevens van de gebruikers- en beveiligingsgroepen uit jouw eigen Active Directory over te nemen.

Je kan kiezen om de gebruikers een pincode als extra wachtwoord in te laten voeren bij het inloggen. Deze ontvangen ze als sms op hun mobiele telefoon. Dit is een extra betaalde dienst die je kunt afnemen als je extra beveiliging wilt. Microsoft ondersteunt ook andere beveiligingsoplossingen van diverse leveranciers.

Met behulp van Data Loss Prevention kan je voorkomen dat bepaalde gevoelige informatie door collega's per ongeluk verstuurd wordt in een e-mail of in de bijlage. Met behulp van Information Rights Management Service kan je jouw gebruikers de mogelijkheid geven om bepaalde e-mails versleuteld te versturen. De ontvangers van deze e-mail kunnen vervolgens de e-mail alleen lezen en niet afdrukken of doorsturen.

6. Hoe veilig zijn mijn gegevens in Office 365?

Bepaal zelf hoeveel je wilt investeren in maatregelen om mogelijke inbreuk op de beveiliging en privacy van jouw gegevens tegen te gaan. Maar blijf wel reëel, want bij elk medium met verbinding naar het internet kan worden ingebroken. Dat kan dan ook in jouw eigen omgeving gebeuren.

Microsoft biedt standaard een robuuste en veilige omgeving met Office 365 voor e-mail en gegevensopslag en investeert continu om dit te waarborgen. Voor de meesten zijn de standaard instellingen in Office 365 zelfs al voldoende. Zo niet, dan kan je de veiligheids- en privacy-instellingen aanpassen aan jouw eisen. Veel van deze instellingen zitten in de basisversie, andere zitten in de geavanceerde versie, als extra dienst of door een koppeling met jouw eigen netwerk.

Office 365-klanten kunnen vertrouwen op Microsoft voor de beveiliging van hun gegevens en de bescherming van de privacy en beveiliging van klantgegevens en is continu bezig om uw vertrouwen te winnen. Uitgebreide informatie vind je op de Office 365 Vertrouwenscentrum pagina op de website van Microsoft.

Over Paradigit Zakelijk

Als strategisch partner voor zakelijke relaties biedt Paradigit Zakelijk zorgeloos werken met Remcoh. Remcoh neemt alle zorgen op het gebied van automatisering én systeembeheer uit handen. Paradigit zakelijk is dé specialist in het opleveren van turnkey projecten, het leveren van deskundig advies en biedt tevens een ruim aanbod van computers, servers, storage- en netwerkapparatuur voor uw bedrijfsnetwerk.

Contact

Indien u vragen heeft kunt u contact opnemen met Paradigit zakelijk.

Paradigit Zakelijk
Hooge Zijde 30
5626 DC Eindhoven
Tel: 040-7512100
Fax: 040-7512199

E-mail: info@remcoh.nl